Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A communication device, comprising:

an executing unit configured to execute software;

a memory configured to store permission data, the permission data indicating permissible behavior for an application, the application being a group of functions provided by execution of the software;

a checking unit configured to check, by accessing an external device before the software is executed, whether the permission data are valid; and

an execution control unit configured to:

permit the executing unit to execute the software when, on the basis of a result of the check carried out by the checking unit, the permission data are determined to be valid, and when, on the basis of the permission data, that the software to be executed is determined to include permissible behavior, and;

~~for not permitting~~ not permit the executing unit to execute the software when, on the basis of the result of the check executed by the checking unit, the permission data are determined to be invalid or when, on the basis of the permission data, that the software to be executed is determined not to include permissible behavior.

2. (Previously Presented) A communication device according to claim 1, further comprising,

a determining unit configured to determine whether it is necessary to carry out the check by the checking unit, the checking unit either carrying out or not carrying out the check on the basis of a determination made by the determining unit.

3. (Previously Presented) A communication device according to claim 2, wherein, the determining unit comprises:

a counting unit configured to count a number of executions of the software; and

a frequency data memory configured to store frequency data indicating how frequently it is necessary to carry out the check; and wherein,

the determining unit is configured to determine, on the basis of a number of executions of the software, as counted by the counting unit, and on the basis of the frequency data stored in the frequency data memory, whether it is necessary to carry out a check by the checking unit.

4. (Previously Presented) A communication device according to claim 2, wherein, the determining unit comprises:

a timer configured to provide time data indicating a present time; and

a time interval data memory for storing time interval data indicating a time interval at which it is necessary to carry out the check; and wherein,

the determining unit is configured to calculate, on the basis of time data provided by the timer, a time period between a present time and a time recorded at a most recent execution of the software, and determines whether it is necessary to carry out the check by the checking unit on the basis of the calculated time period and the time interval data stored in said time interval data memory.

5. (Previously Presented) A communication device according to claim 1, further comprising:

a count data memory configured to store count data indicating a number of times that the software is allowed to be executed in a condition that the checking unit is unable to make the check; and

the execution control unit is configured to permit the executing unit to execute the software in a condition that the checking unit is unable to make the check up to a number of times which is indicated by the count data stored in the count data memory.

6. (Previously Presented) A communication device according to claim 1, further comprising:

an updating unit configured to obtain update data from the external device, and updating the permission data stored in the memory on the basis of the update data.

7. (Previously Presented) A communication device according to claim 6, wherein:

the updating unit is configured to:

transmit, to the external device, update timing data indicating a timing of a most recent update of the permission data stored in the memory, when the checking unit makes the check;

receive update data transmitted from the external device in response to the transmission of the update timing data; and

update the permission data stored in the memory on the basis of the update data.

8. (Previously Presented) A communication device according to claim 1, further comprising:

a terminating unit configured to instruct the executing unit to terminate execution of the software when the application attempts to conduct behavior which the application is not permitted to conduct.

9. (Previously Presented) A communication device according to claim 1, wherein:

the permission data contain information on usage of at least one of an internal hardware resource of the communication device, an external hardware resource of the communication device, a software resource and a communication network resource.

10. (Currently Amended) A method for controlling a communication device, the method comprising:

transmitting to the communication device permission data, the permission data indicating permissible behavior for an application, the application being a group of functions provided by execution of software in the communication device;

checking, by communicating data between the communication device and an external device, whether the permission data are valid, before the software is executed in the communication device; [[and]]

permitting the software to be executed only when the permission data are determined to be valid on the basis of a result of the check and when the software to be executed is determined to include permissible behavior on the basis of the permission data, and

disallowing the executing unit to execute the software when, on the basis of the result of the check executed by the checking unit, the permission data are determined to be invalid or when, on the basis of the permission data, that the software to be executed is determined not to include permissible behavior.

11. (Currently Amended) A computer readable storage medium storing a program for causing a computer to execute a process, the process comprising:

storing, in a memory, permission data indicating permissible behavior for an application, the application being a group of functions provided by execution of software;

checking, by accessing an external device, whether the permission data are valid, before the software is executed; [[and]]

permitting the software to be executed only when the permission data are determined to be valid on the basis of a result of the check and when the software to be executed is determined to include permissible behavior on the basis of the permission data; and

disallowing the software to be executed when, on the basis of the result of the check, the permission data are determined to be invalid or when, on the basis of the permission data, that the software to be executed is determined not to include permissible behavior.

12. (Currently Amended) A communication method in a communication system comprising (a) a software data providing server device which stores software data containing software for providing a group of functions forming an application, (b) a management server device which stores security descriptor data containing permission data indicating permissible behavior for the application, and (c) an application descriptor data providing server device which stores application descriptor data indicating a storage location of the software data and a storage location of the security descriptor data, the method comprising:

transmitting the application descriptor data from said communication system to said communication device;

transmitting data indicating the storage location of the security descriptor data contained in the application descriptor data from said communication device to said communication system;

transmitting the security descriptor data from said communication system to said communication device on the basis of the data indicating the storage location of the security descriptor data;

storing the security descriptor data in said communication device;

transmitting data indicating the storage location of the software data contained in the security descriptor data from said communication device to said communication system;

transmitting the software data from said communication system to said communication device on the basis of the data indicating the storage location of the software data;

installing, in said communication device, the software contained in the software data transmitted from said communication system to said communication device;

checking, by communicating data between said communication device and said communication system before the software is executed in said communication device, whether the security descriptor data stored in said communication device are valid; [[and]]

permitting said software to be executed in said communication device only when the security descriptor data are determined to be valid on the basis of a result of the check and when the software to be executed is determined to include permissible behavior on the basis of the permission data; and

disallowing the software to be executed in said communication device when the security descriptor data are determined to be invalid on the basis of the result of the check or when, on the basis of the permission data, that the software to be executed is determined not to include permissible behavior.

13. (Previously Presented) A communication device according to claim 1, wherein the application comprises a Java application; and

wherein the permission data comprises a scope of rights which are granted to the Java application.

14. (Previously Presented) A communication device according to claim 1, wherein the permission data indicates that the application is allowed to access information designated as confidential.

15. (Previously Presented) A communication device according to claim 1, wherein the permission data indicates that the application is allowed to access telephone directory information.

16. (Previously Presented) A communication device according to claim 1, wherein permission data indicates that the application is allowed to access e-mail information.

17. (Previously Presented) A communication device according to claim 1, wherein permission data indicates that the application is allowed to reconfigure the communication device.

18. (Previously Presented) A communication device according to claim 1, wherein permission data indicates that the application is allowed to access configuration information relating to the communication device.

19. (Previously Presented) The method according to claim 10, wherein the permission data indicates that the application is allowed to access information designated as confidential.

20. (Previously Presented) The computer readable storage medium according to claim 11, wherein the permission data indicates that the application is allowed to access information designated as confidential.

21. (Previously Presented) The method according to claim 12, wherein the permission data indicates that the application is allowed to access information designated as confidential.